State of California
Office of the State Chief Information Officer
Office of Technology Services

Standard

Owner: Security Management Division

Number: 3117
Issue Date: 01/28/2008
Revised: 11/10/2009

NETWORK ARCHITECTURE STANDARD

Section 1 – Introduction

The Office of the State Chief Information Officer (OCIO), Office of Technology Services (OTech) Security Management Division (SMD) requires that systems hosted and supported by OTech in the hosting environment be designed to follow an "n-tiered" network architecture. "N-tier architecture" is characterized by the functional decomposition of applications, service components, and their distributed deployment. A "tier" is a functionally-separated hardware and software component. Typically, n-tier architectural platforms place each service, or group of services, on a separate server, enabling systems to be divided into easily-scalable components. The most widespread use of "multi-tier architecture" refers to three-tier architecture. This Standard defines the requirements surrounding the components of n-tiered architecture and the acceptable tiered architectural designs. This Standard applies to environments that contain confidential, sensitive, and/or personally identifiable data.

IMPORTANT: System data in the hosted environment must be classified by the customer and disclosed to OTech staff; specifically the customer representative and/or account manager. Hosted systems containing unclassified data will adopt the most restrictive security measures by default.

Section 2 – Standard Requirements

This section provides a high-level description of the web, application, and data tiers and the acceptable tiered network architecture designs.

A. Network Architecture Tiers

1. De-Militarized Zone (DMZ)
   The De-Militarized Zone (DMZ), sometimes called the web tier or web layer, is the top-most level of the application. The OTech will use a system of physical and logical firewalls to create a DMZ. A DMZ is a sub-network (or set of networks) that resides between a trusted internal network, such as the OTech internal network, and an untrusted external network, such as the public Internet. It is used to provide services to the outside world without allowing the outside world directly into the internal network.

   a) Listed below are system components that ***must*** reside in a DMZ:
      - Public-facing web servers
      - Publicly accessible File Transfer Protocol (FTP) servers. Windows 2008 operating systems or later must use Secure FTP instead of FTP.
      - Proxy servers

- Email gateways
- Streaming Video servers that only stream public information
- Incoming fax servers and incoming/outgoing fax servers
- Public-facing Domain Name System (DNS) servers
- Traffic management and security components that permit the above devices to function effectively and securely

2. Application Tier
   The application tier, sometimes referred to as the logic/business logic layer, logically resides between the DMZ and the data tier. This tier is responsible for accessing the data tier to retrieve, modify and/or delete data to and from the data tier and send the results to the devices in the DMZ (web tier). This tier also controls an application's functionality by performing detailed processing.

   a) Listed below are system components that may reside in the application tier:
      - Applications or application servers
      - Authentication devices, such as active directory or domain controllers
      - Devices processing information
      - Non-public facing FTP servers
      - Non-public facing web servers hosting Intranet (internal) applications
      - Internal DNS servers
      - Outgoing fax servers (isolated within this tier)
      - Project specific traffic management and security components that permit the above devices to function effectively and securely

   b) No direct public access is allowed to the application tier.

3) Data Tier
   The data tier, sometimes referred to as the database tier or intranet zone, is the inner- most tier of the n-tier architecture. This tier hosts databases and database servers that store and retrieve information. This tier keeps data neutral and independent from application servers and business logic. Giving data its own tier improves scalability and performance in addition to minimizing the risk of unauthorized access attempts.

   a) Listed below are system components that may reside in the data tier:
      - Databases, database servers, and file servers
      - Storage area networks and network attached storage
      - Internal DNS servers
      - Database archive and reporting servers
      - Devices storing confidential or sensitive information

   b) No direct public access is allowed to the data tier.

B. Standard Network Architectures

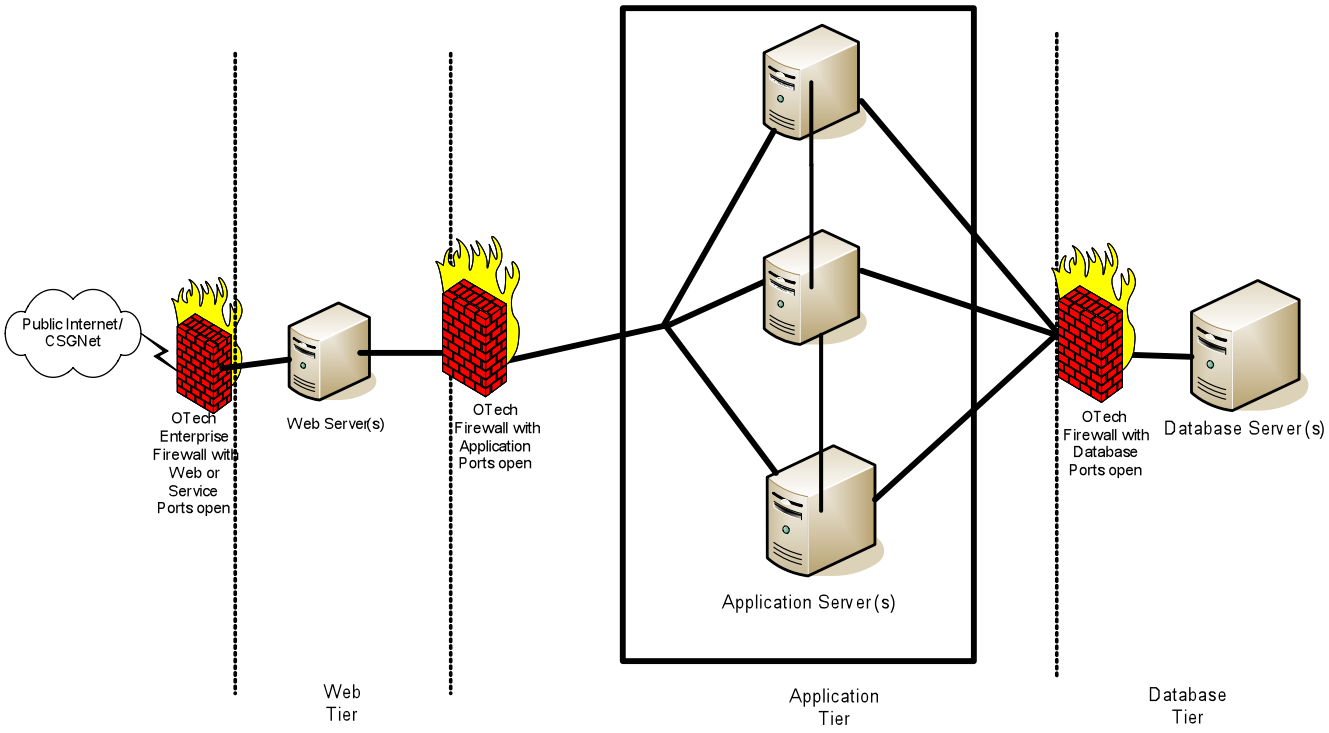
The SMD requires that systems be designed to one of the two network architectures (Three-Tier or zOS Architecture) listed below. If either of these designations cannot be applied, please refer to Section 3 of this Standard.

1. Three-Tier Architecture
   Separation of the three functional tiers is the preferred architecture design. Separating the web server(s), application server(s), and database server(s) is the best way to isolate the most vulnerable devices from the more sensitive devices—creating the most layers of difficulty to compromise system data.

Firewall with Public-Facing Web Service Ports Open	**DMZ**	Firewall with Application Ports Open	**Application Tier**	Firewall with Database Ports Open	**Data Tier**

Provided below is a simplified **sample** three-tier network architecture diagram:

Sample Three-Tier Network Architecture



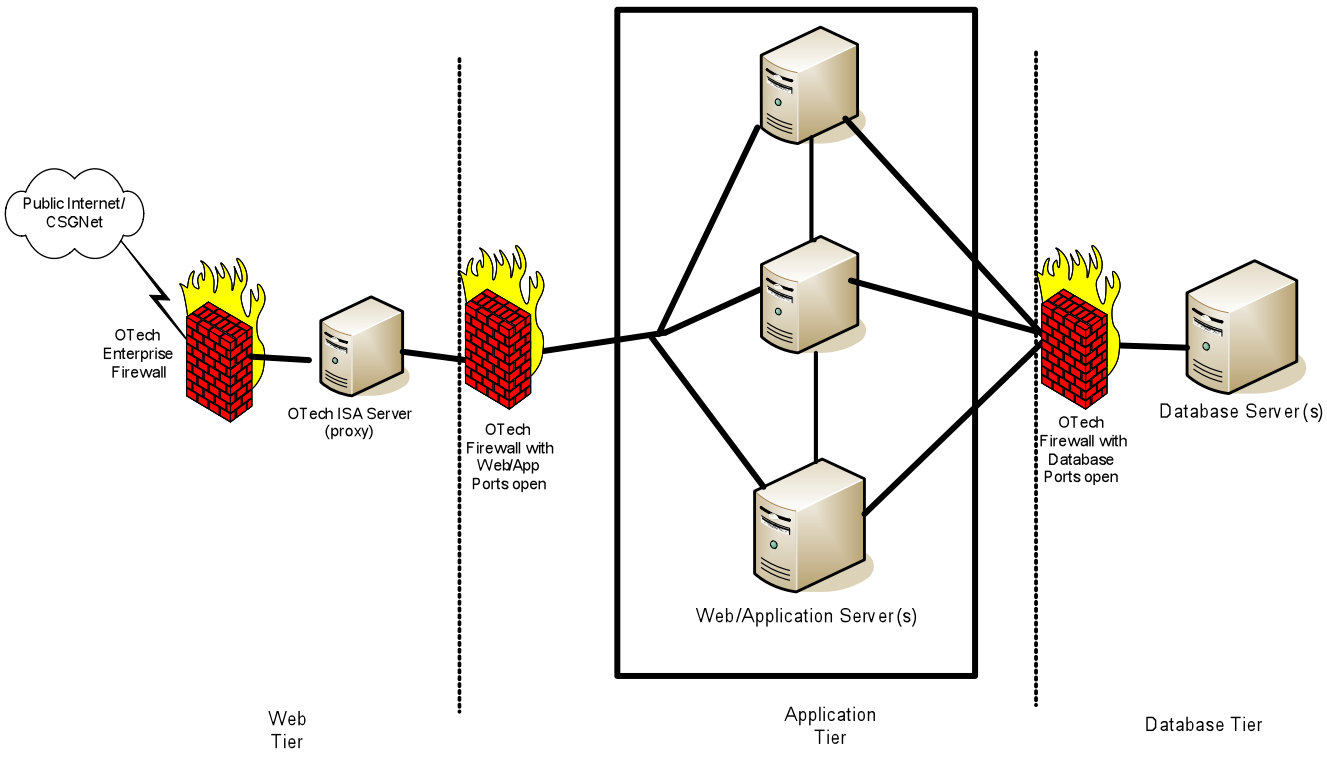
Separation of the combined web/application function(s) from the data function(s). Application requirements to combine the functions of the web server(s) and application server(s) onto one physical device is permitted so long as the system utilizes a proxy. The proxy separates the enterprise network from the outside network. A proxy is a server (a computer system or an application program) that services the requests of its clients by forwarding requests to other servers, as opposed to allowing the client requests direct access to another server. A client connects to the proxy, requesting some service available from a different server. The proxy provides the resource by connecting to the

specified server and requesting the service on behalf of the client. Since no direct public access is allowed beyond the DMZ, a proxy must be used.

Firewall with Public-Facing Web Service Ports Open	**Proxy**	Firewall with Web Ports Open	**DMZ & Application Tier**	Firewall with Database Ports Open	**Data Tier**

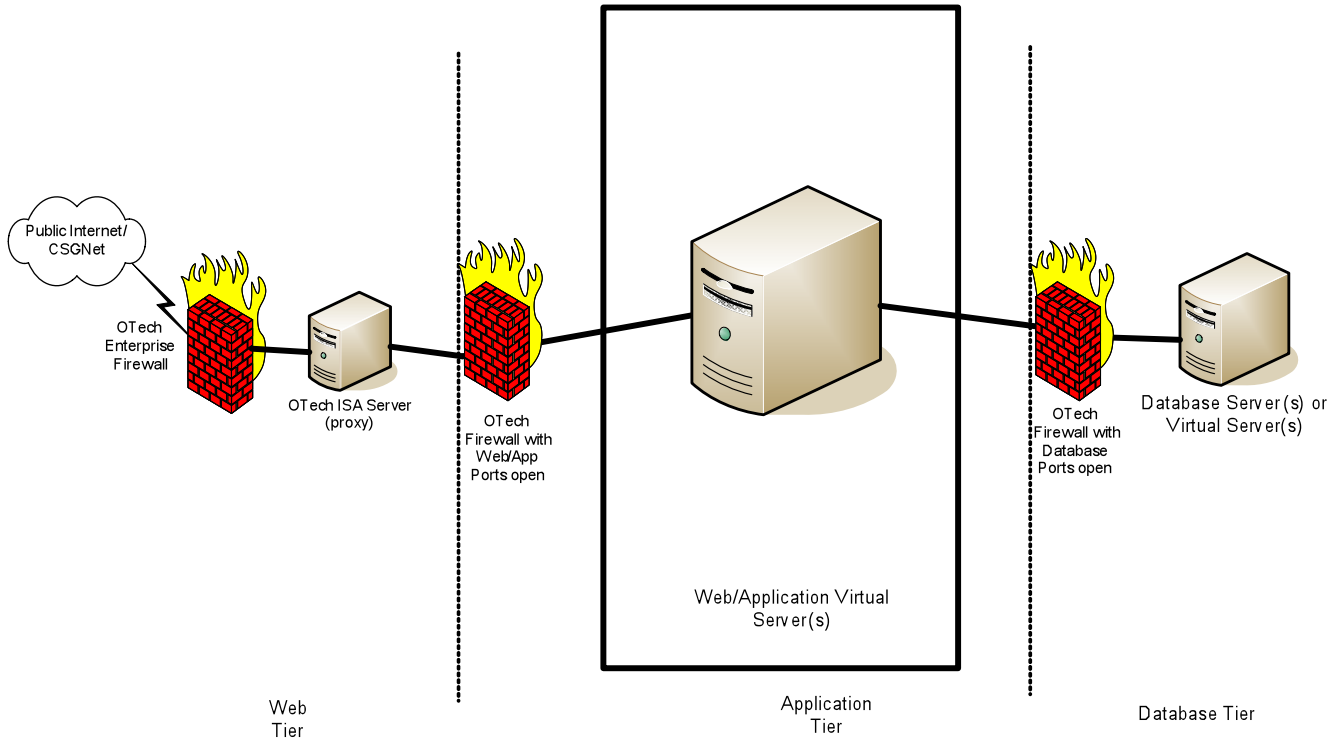
Provided below is a simplified **sample** three-tier network architecture diagram:

Sample Three-Tier Network Architecture with ISA



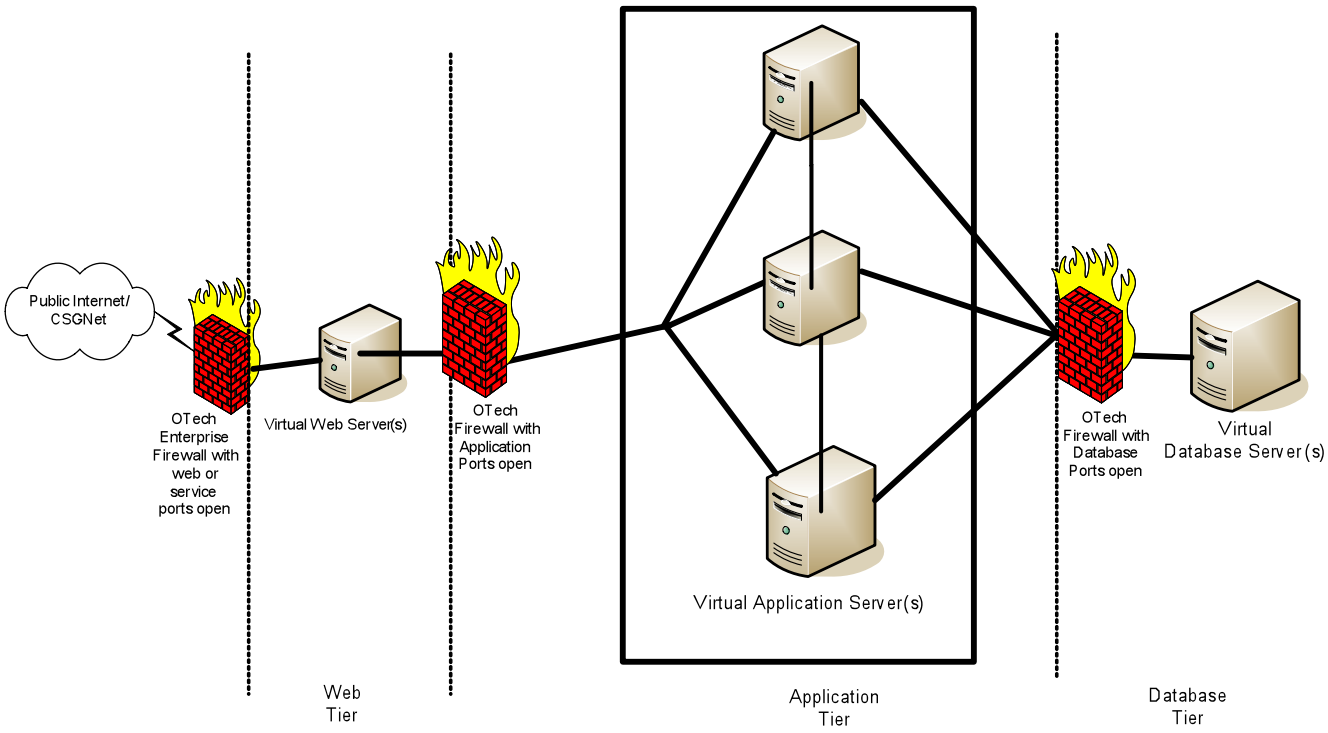
Provided below is a simplified **sample** three-tier network architecture diagram including virtual servers:

Sample Three-Tier Network Architecture



Provided below is a simplified **sample** three-tier network architecture diagram including virtual servers:

Sample Three-Tier Network Architecture

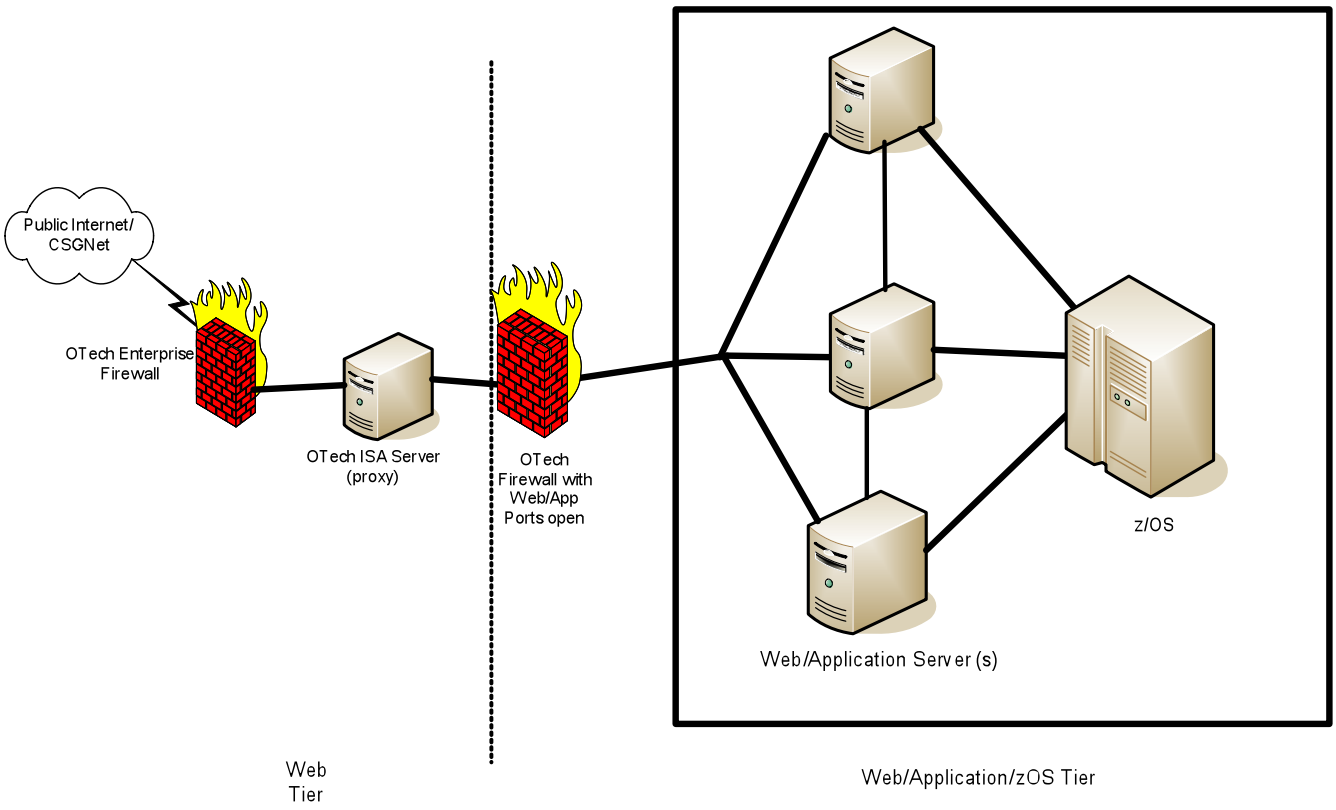


2. z/OS Architecture
   Combination of the web/application/data functions in one tier **ONLY** if housed on z/OS system(s) and a proxy is used. Since no direct public access is allowed beyond the DMZ, a proxy must be used. z/OS features and facilities provide a high level of security and system integrity specifically designed to protect one program from affecting another, either intentionally or accidentally. Facilities such as System Authorization Facility (SAF), Resource Access Control Facility (RACF), and Authorized Program Facility (APF) in addition to system integrity features, such as storage protection and cross-memory communication controls, warrant this design.

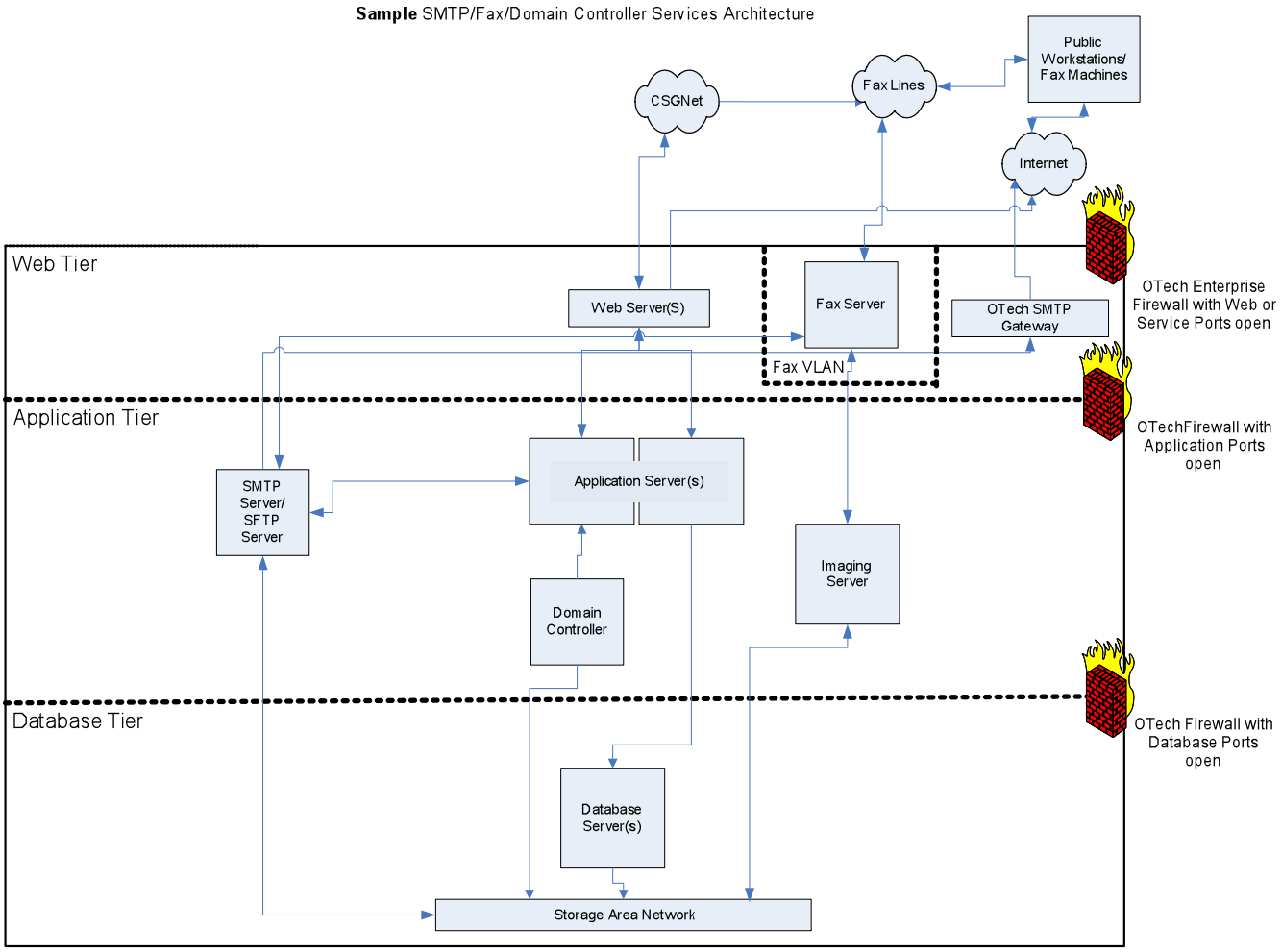
Firewall with Public-Facing Web Service Ports Open	**Proxy**	Firewall Application Ports Open	**DMZ & Application & Data Tier ONLY for z/OS**

Provided below is a simplified **sample** z/OS tier network architecture diagram:

Sample z/OS Network Architecture

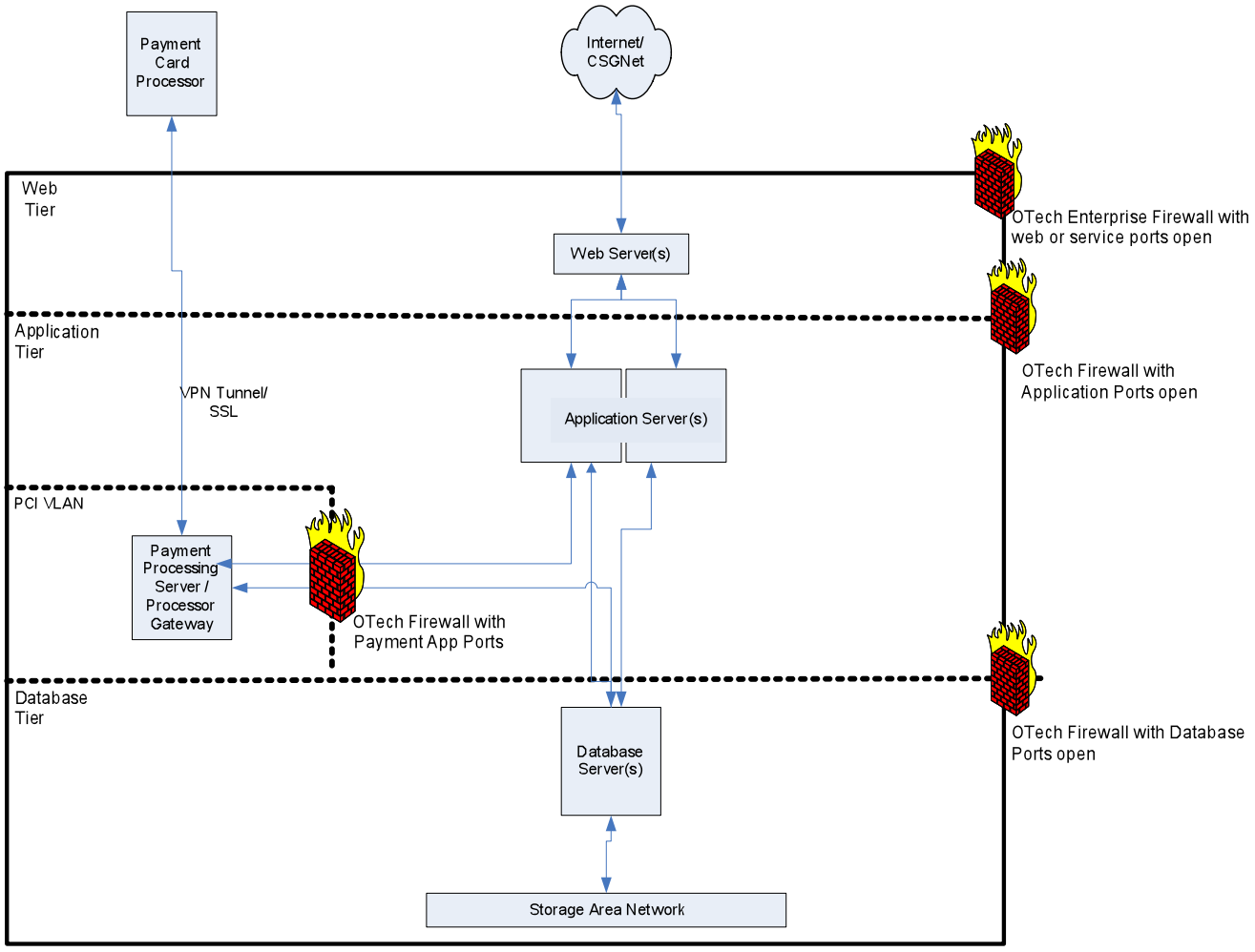


Provided below is a simplified **sample** three-tier network architecture diagram that includes common IT services such as SMTP, fax, and authentication services:



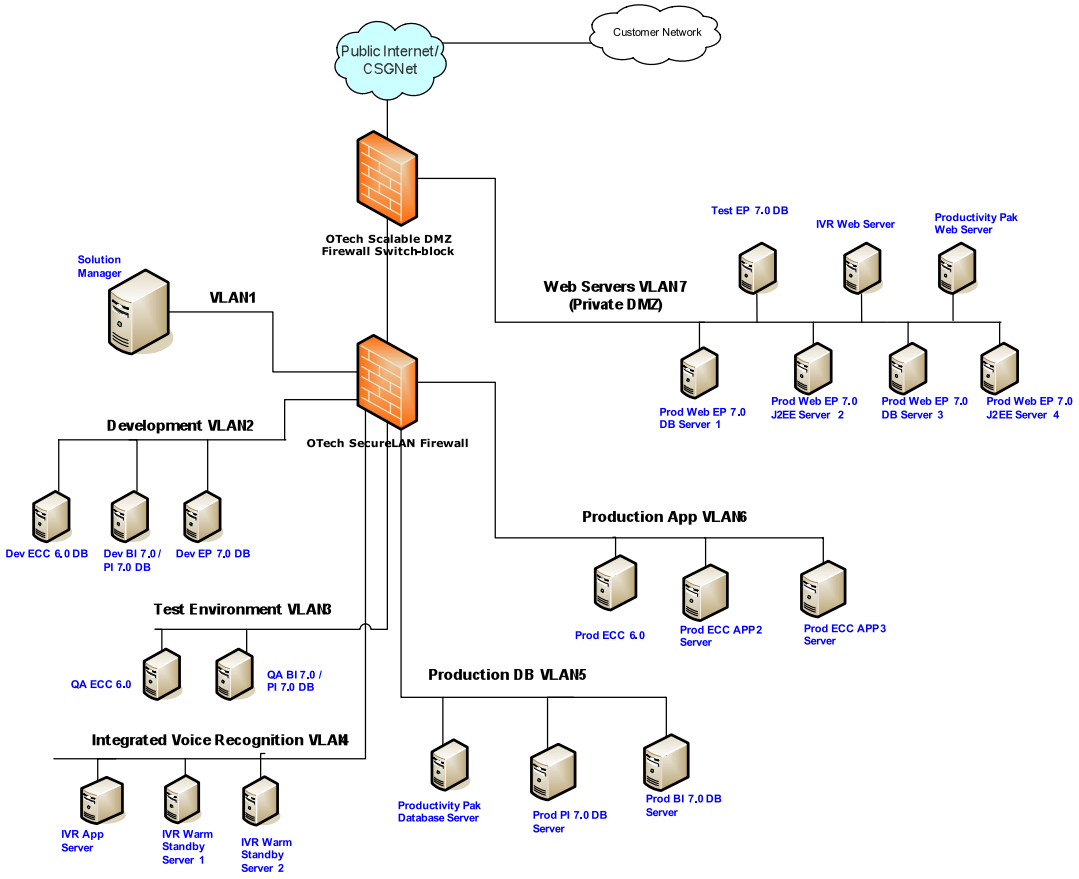
Provided below is a simplified **sample** n-tier network architecture diagram that adheres to the Payment Card Industry (PCI) Data Security Standards (DSS). Applications that process, store, or transmit payment card data must adhere to PCI-DSS.

Sample Payment Card Industry (PCI) Architecture



3. Multi-Environment Architectures
   Multiple environments (development, test, pre-production, production) may not exist on the same virtual local area network (VLAN). They must be separated by a firewall. Provided below is a simplified **sample** network architecture diagram that includes multiple environments:

Sample Multi-Environment Architecture



Section 3 – Applicability and Exclusions

A. This Standard applies to applicable customer or OTech systems hosted in the managed services environment.

Intranet web service applications via CSGNet are not held to the above architectural requirements.

This Standard does ***not*** apply to Customer Owned Equipment Managed Service (COEMS).

This Standard does not apply to development-only environments where no confidential, sensitive, and/or personally identifiable information is processed, stored, or transmitted and is not publicly accessible.

Direct any questions regarding the applicability of this Standard to the Security Management Division for clarification.

B. Exceptions to this Standard must be documented and will be considered on a case-by-case basis. Requests for an exception to this Standard must be submitted via the Security Policy/Procedure Exception Request Form, OCIO 358.

Section 4 – Auditing and Reporting

A. Auditing may be performed on a periodic or random basis by the Security Management Division or its designees. In the event an audit determines this Standard is not being applied, notification will be sent to the appropriate person for remediation.

B. Any known violations of this Standard must be reported to the OTech Chief Information Security Officer and the reporting employee's immediate supervisor.

Section 5 – Authority/References

3100 - Acceptable Use Policy
Security Policy/Procedure Exception Request Form, OCIO 358